



**FUNCTIONAL SAFETY ENGINEER  
CERTIFICATION COURSE  
IN  
SAFETY INSTRUMENTED SYSTEMS  
IEC 61511 AND IEC 61508**

Slide 1- 1



**Objective of the FSE Certification Course**

To provide attendees with a fundamental understanding of the principles of functional safety according to IEC 61511 and IEC 61508 with respect to the design and management of Safety Instrumented Systems (SIS) in the process industry

To assess the competency of the attendees by exam as the first step towards registration and certification in the TÜV Rheinland Functional Safety Program

Slide 1- 2



## Function Safety Engineering

### Introductions

#### Welcome to the workshop

- **My background and experience**
- **About you?**
  - Your Name
  - A little background
  - What to do you want out of this Course
  - What does your company want out of this course

Slide 1- 3



## Function Safety Engineering

### ■ Workshop Facilities & Etiquette

- In case of an emergency – exits and alarms
- Toilets - location
- Breaks – formal & feel free to stretch at any time
- Tea & Coffee – help yourselves at any time
- Feel free to ask questions at anytime
- Please set mobile phones to silent so it doesn't effect your colleagues

Slide 1- 4



## Function Safety Engineering

- **Duration**
  - 3 day course with homework
  - Exam on fourth day
- **Exam**
  - ◆ Four hour two part exam
  - ◆ Part 1 – 60 multiple choice questions
  - ◆ Part 2 – 10 Open question
- **Working day**
  - 09:00 – 17:00
  - Lunch at 12:30 – 13:30

Slide 1- 5



## Function Safety Engineering

### FSE Course Contents

- Introduction to IEC 61508 and IEC 61511
- Functional Safety Management and the Lifecycle
- Competency Management and Assessment
- Process Hazard and Risk Assessment
- Risk Reduction and Safety Allocation
- Safety Requirements Specification
- Design and Development of the Safety Instrumented Function
- Software for Safety
- Safety Integrity Level Verification Calculation Methods
- Safety Integrity Level Determination
- SIL Determination for Fire and Gas Systems (ISA Methodology)
- Operations & Maintenance
- Exam

Slide 1- 6



## Function Safety Engineering

### Today

- Introduction to IEC 61508 and IEC 61511
- Functional Safety Management and the Lifecycle
- Competency Management and Assessment
- Hazard and Risk Assessment
- Risk Reduction and Safety Allocation
- Safety Requirements Specification

Slide 1- 7



## Function Safety Engineering

### Day 2

- Design and Development of the SIF
- Software for Safety
- Understanding Failure
- Failure Data and Sources
- Interpreting Failure Data
- Safety Integrity Level Verification Methods

Slide 1- 8



## Function Safety Engineering

### Day 3

- Safety Integrity Level Determination
  - ◆ Risk Graphs
  - ◆ Layers Of Protection Analysis
- SIL Determination for Fire and Gas Systems
- Operations and Maintenance
- Exam Preparation

Slide 1- 9



## Function Safety Engineering

### Introduction to Functional Safety

Slide 1- 10



## What is Safety

- The condition of being safe
- Freedom from danger, risk, or injury
- Freedom from unacceptable risk
- Safety is the state of being "safe" (from Latin *Salus*)
- The condition of being protected from harm or any other event which could be considered non-desirable.

Slide 1- 11



## What is Functional Safety (IEC 61511)

A part of the overall Process Safety approach

IEC61511-1 clause: 3.2.25

Part of the overall safety relating to the process and the Basic Process Control System which depends on the correct functioning of the Safety Instrumented System and other protection layers

Slide 1- 12

## **What is Functional Safety?**

- A safety system is functionally safe if:
  - Random, common cause and systematic failures do not lead to malfunctioning of the safety system resulting in:
    - Injury or death of humans
    - Spills to the environment
    - Loss of equipment or production

Slide 1- 13

## **Challenges in Achieving Functional Safety**

The challenge is to design a system in such away as to prevent dangerous failures or to control them when they arise from:

- Incorrect specifications of hardware or software
- Omissions in the safety requirements specification
- Random hardware failure mechanisms
- Systematic hardware failure mechanisms
- Software errors
- Common cause failures
- Human error
- Environmental influences
- Supply system voltage disturbances

**One of the key concepts to achieving FS is Safety Integrity Levels**

Slide 1- 14

## What is the Safety Integrity Level (SIL)

- SIL is a:
  - ◆ Qualitative measure of safety integrity in terms of the avoidance of systematic failures
  - ◆ Quantitative measure of safety integrity in terms of the hardware failures and fault tolerance
  - ◆ One of four levels of integrity
  - ◆ An order of magnitude risk reduction against a single hazard occurrence
- *SIL is not just an assessment of the loop hardware*

Slide 1- 15

## Safety Integrity Level

- Three important SIL properties to remember
  - ◆ Includes all of the safety instrumented function
  - ◆ The higher the SIL the more robust the requirements to achieve it
  - ◆ Includes hardware and systematic requirements

**IEC 61511 Table 3 – Safety Integrity Levels: Probability of Failure on Demand (Demand Mode of Operation)**

Safety Integrity Level (SIL)	Target average probability of failure on demand	Target Risk Reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10,000$ - $\leq 100,000$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 1000$ - $\leq 10,000$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 100$ - $\leq 1000$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10$ - $\leq 100$

Slide 1- 16



## Safety Integrity Levels Continued

IEC 61511 Table 4 – Safety Integrity Levels: frequency of dangerous failures of the Safety Instrumented Function  
(Continuous Mode of Operation)

Safety Integrity Level (SIL)	Target frequency of dangerous failures to perform the safety instrumented function (per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Slide 1- 17

## What is Functional Safety Engineering -

- Hazard Identification – Consequence / Frequency Analysis
- Targets of Tolerability / Acceptability of Risk – Safety Targets
- Risk Assessment / Risk Reduction / Safety Integrity Levels
- Engineering / Management Capability to a target Safety Integrity
- Lifecycle Processes to a target Safety Integrity
- Verification / Validation to a target Safety Integrity
- Understanding Change Management

FSE requires a Multi disciplined Approach to Safety

Slide 1- 18



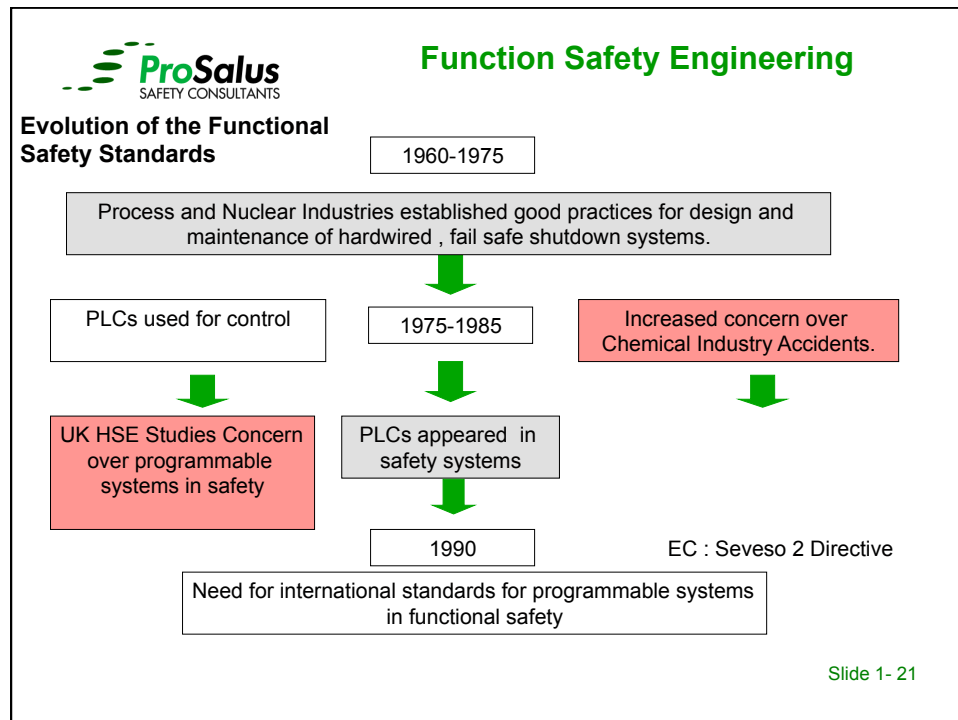
## **Introduction to the Functional Safety Standards**

Slide 1- 19



- Some guidance was available on designing instrument protective functions, ICI, Shell, BP etc
- Systematic issues not included in guidance
- Replacement of relays and solid state logic with software based logic systems raised issues with:
  - How to decide what systematic integrity was required
  - How to achieve and maintain required Hardware and software integrity
  - What had to be considered to achieve systematic integrity

Slide 1- 20



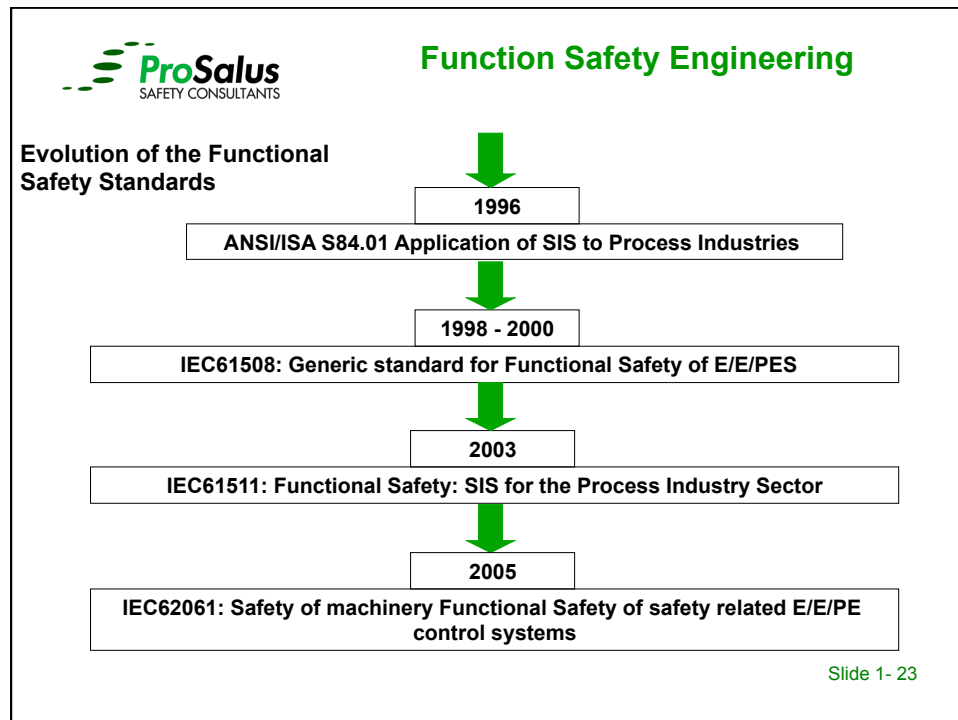
**ProSalus**  
SAFETY CONSULTANTS

### Function Safety Engineering

#### Need for Internationally recognised standard for E/E/PES

- By 1990: An urgent need for guidance, standard or code of practice for Functional Safety Engineering – SIS.
- Existing practice was based on solid state and German DIN 19250 with no provision for programmable systems.
- Systematic requirements not clearly identified
- Process Safety Management and Regulation changes include assessment and auditing of safety measures including Safety Instrumented Systems

Slide 1- 22

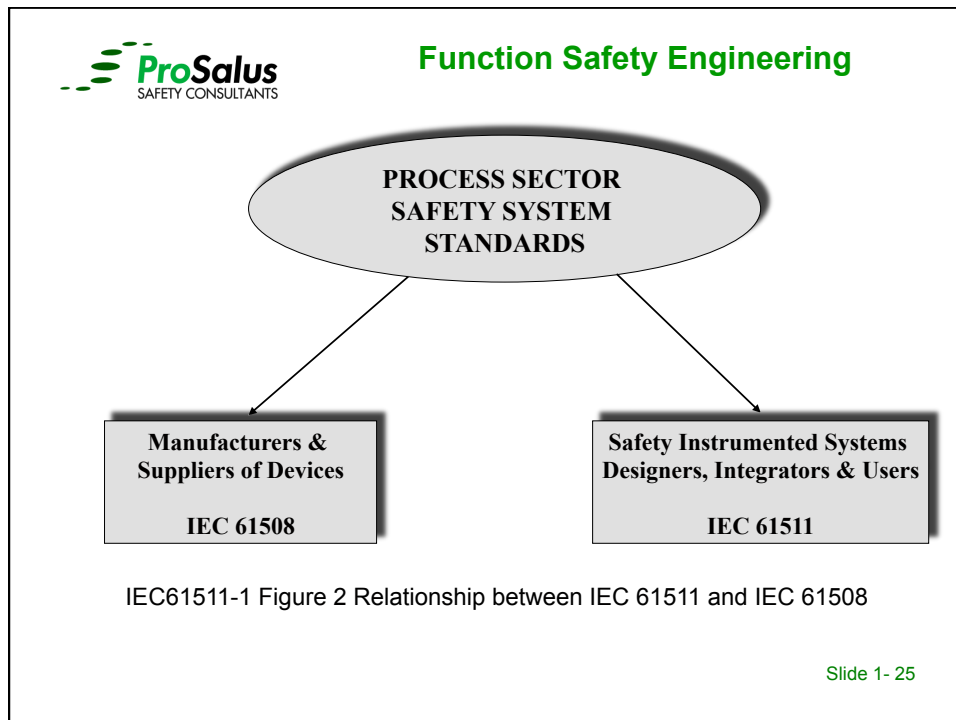



 **Function Safety Engineering**

**Functional Safety Standards used in the Process Industry**

- **IEC 61508:** Functional safety of electrical/electronic / programmable electronic safety-related systems
- **IEC 61511 / ANSI/ISA 84.00.01 Modified:** Functional Safety: safety instrumented systems for the process industry sector
- **IEC 62061:** Safety of Machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- **ISO 13849:** Safety of Machinery – Safety-related parts of control systems – General principles of design and validation
- **EN 50402:** Functional Safety requirements for fixed gas detection systems
- **ISO 13702:** Requirements and guidelines for the control and mitigation of fire and explosions on off-shore oil and gas installations
- **ISO 10418:** Analysis, design, installation and testing of surface protection systems

Slide 1- 24



 **Function Safety Engineering**

**IEC 61508**

**Title: Functional safety of electrical/electronic/programmable electronic safety-related systems –**

- Part 0: Introduction to functional safety
- Part 1: General requirements
- Part 2: Requirements for electrical / electronic /programmable electronic systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 65108-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

Slide 1- 26



## Function Safety Engineering

### **IEC 61508 Generic Standard for all Industry Applications**

#### **The Scope of IEC 61508 applies to:**

- Any safety related device or system based on electrical/ electronic / programmable electronic (E/E/PE) Technology
- Any Safety related systems in any industry sector including Process, Nuclear, Oil & Gas, Exploration, Sub Sea, Aerospace, Military , Railway, Motor Industry, Shipping e.g. pipe laying vessels etc
- Industries where no sector specific functional safety standard exists
- Applicable World wide (subject to individual country acceptance)

Slide 1- 27



## Function Safety Engineering

### **IEC 61511**

#### **Title: Functional Safety- Safety Instrumented Systems for the Process Industry Sector**

Part 1: Framework, definitions, system hardware and software requirements

Part 2: Guidelines for the application of IEC 61511-1

Part 3: Guidance for the determination of the required Safety Integrity Levels

Slide 1- 28



## Function Safety Engineering

### IEC 61511

Part 1: Mandatory requirements for work procedures, records, hardware, software, testing, maintenance, assessment. Based on safety lifecycle framework.

Part 2: Extensive guidance on Part 1 - methods and design features to achieve required levels of safety integrity.

Part 3: Guidance on methods of determining the required Safety Integrity Level for any Safety Instrumented Function. Quantitative (e.g. FTA method), Semi Quantative (e.g LOPA method) and qualitative methods (e.g. risk graph method).

Slide 1- 29



## Function Safety Engineering

### IEC 61511 Functional Safety for the Process Industry Sector

#### The Scope of IEC 61511 applies to:

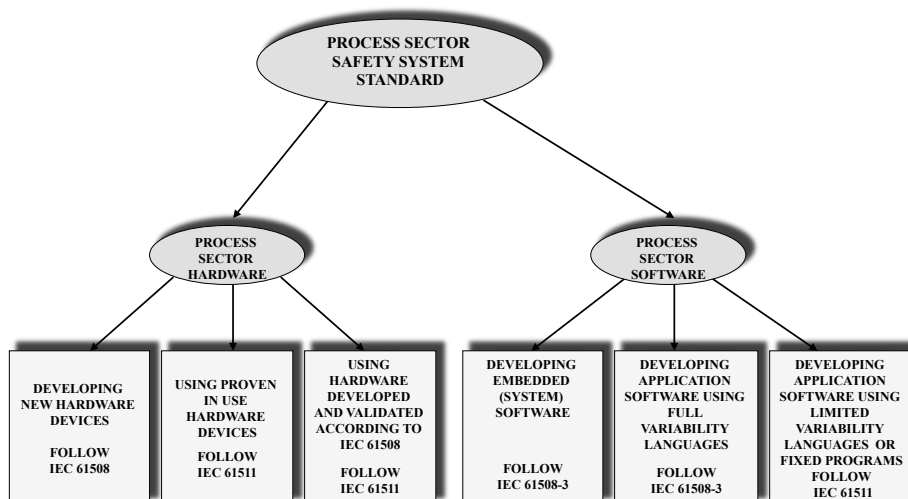
- Chemicals, Tank Storage, Pharmaceutical, Non Nuclear Power, Utilities Industry, Oil and Gas Production and Exploration, Bio Plants.....
- Safety Instrumented Systems – normally pre certified / approved / assessed
- Legacy Safety Instrumented Systems
- Pipe to Pipe Standard (Sensor to Final Element)
- Excludes Operating, Source and Embedded Software (Full Variability Language FVL)
- Not for device certification
- ANSI/ISA 84.00.01-2004 (IEC 61511 Modified) USA implementation with Grandfather clause

Slide 1- 30

**Additional Informative Guidance:-**

- ◆ EEMUA 222 – Guide to the Application of IEC 61511 to safety instrumented systems in the UK process industries;
- ◆ Norsok OLF070 – Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry;
- ◆ EI/IP – Guidance on assessing the safety integrity of electrical supply protection;
- ◆ CASS - Guide to Functional Safety Capability Assessment;
- ◆ ISA-TR84.00.02-2002 – Parts 1 to 5 – SIF – SIL Evaluation Techniques;
- ◆ ISA-TR84.00.02-2002 – Guidance for Testing of Process Sector SIFs
- ◆ CDOIF– Guideline Demonstrating Prior Use
- ◆ IChemE – Using risk graphs for SIL Assessment – a user guide for ChemEng
- ◆ EI Draft – Guidance on SIL Determination
- ◆ EI Draft – Guidance on Quantified Human Reliability Analysis

Slide 1- 31

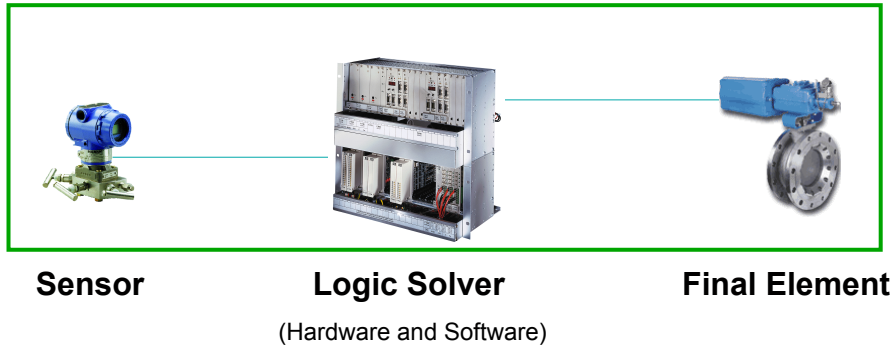


IEC 61511-1 Figure 3 - Relationship between IEC 61511 and IEC 61508

Slide 1- 32



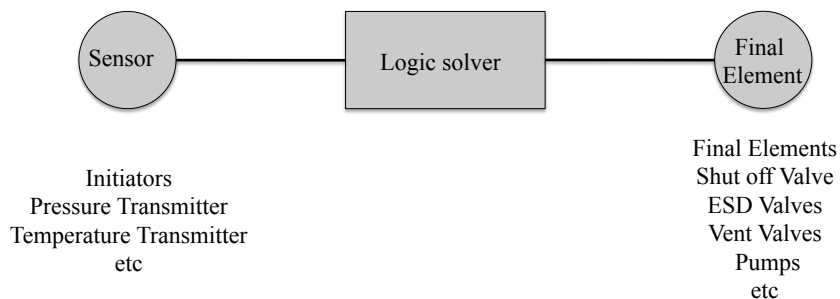
## Scope of a Safety Instrumented Function



Slide 1- 33

## Safety Instrumented Functions

A SIF is always formed from three sub systems



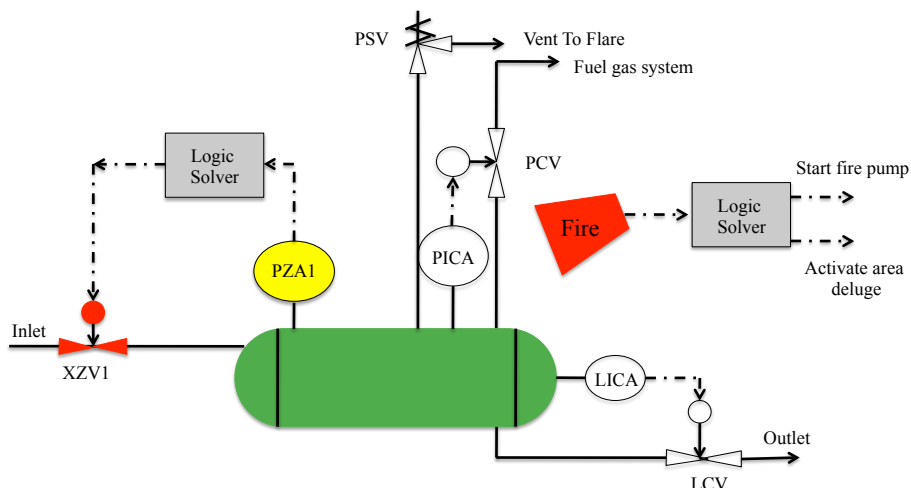
Slide 1- 34

## Safety Instrumented Functions

- Safety Instrumented Systems (SIS) are one of the most widely used active risk reduction techniques that form part of the preventative protection layers
- A SIS is made up of individual Safety Instrumented Functions (SIF)
- A SIF contributes to the overall risk reduction for an identified hazard
- Overall risk reduction is made up of many layers (safeguards) that are identified during the hazard study
- The cause / consequence pair identified during the hazard study helps determine the amount of risk reduction required
- An Instrument SIF helps to prevent / reduce the frequency of a hazardous event
- A F&G SIF helps to mitigate / reduce the consequences of a hazardous event

Slide 1- 35

## Typical Safety Instrumented Functions (Preventative & Mitigative)



Slide 1- 36



## Function Safety Engineering

### Safety Instrumented Functions

A SIF protects against a single hazard is identified during a hazard study

A Safety Instrumented System (SIS) is made up of several SIF loops

A SIF can be:

- a single initiator and several final elements;
- a single final element and several initiators

The SIF Functional, Integrity and logical relationship between Inputs & Outputs is captured in the Safety Requirements Specification (SRS)

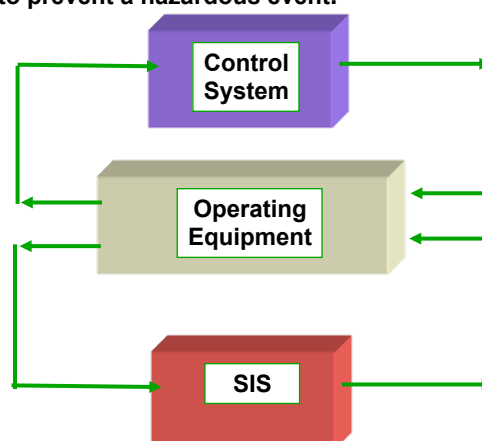
Slide 1- 37



## Function Safety Engineering

**Safety Instrumented Systems act independently of the process or its control system to try to prevent a hazardous event.**

The SIS achieves risk reduction by reducing the frequency (likelihood) of the hazardous event  
The amount of risk reduction allocated to the SIS determines its "target Safety Integrity Level" i.e. SIL



Slide 1- 38

## **Introduction to Regulatory Compliance**

Slide 1- 39

### **So why do we need Functional Safety Standards**

- Because we don't learn from our mistakes
  - ◆ Disasters keeping repeating – Trevor Kletz – “Lessons from Disaster” (ISBN 0 85295 307 0)
- Prescriptive regulations and standards need support from risk / goal based regulations and standards to work effectively when dealing with complexity or novel approaches e.g. API RP 14C
- Latest regulatory approach is risk based goal orientated approach (e.g. In the UK - HASAWA – COMAH – SMS - QRA – Competency)
- A risk based approach needs well trained and competent engineers who are aware and knowledgeable about safety (HSE 2007 – Management of Competency Systems )

Slide 1- 40

### **Hazardous Events that emphasis the need for Safety Standards**

- ◆ **Flixborough, UK, 1974** – Accelerated the introduction of the HASAWA and subsequently the Control of Major Incident Hazards
- ◆ **Seveso, Italy, 1976** – Introduction of the SEVESO Directive I & II  
– Implemented in the UK through the Control OF Major Accident Hazards Regulations (COMAH)
- ◆ **Piper Alpha, UK 1987** – Leads to the HSE taking responsibility for Offshore safety and the introduction of the Offshore Installations (Safety Case) Regulations & Offshore Installations (Prevention of Fire & Explosion, and Emergency Response) Regulations (PFEER)
- ◆ **Buncefield, UK, 2005** – Process Safety Leadership Group (PSLG) Report - Safety & environmental standards for fuel storage sites leading to increased focus on Functional Safety Management

Slide 1- 41

**BP Refinery, Texas City Tx: 23 March 2005**



Slide 1- 42



## Function Safety Engineering

### BP Refinery, Texas City – Refinery Explosion

#### 2010 Agreement between OSHA and BP (Texas City Incident) –

BP shall complete a Safety Instrumented System Lifecycle Management to more completely implement the SIS Standard (ANSI/ISA S84.00.01-2004) at the Refinery and cover the following subject matters:

- (a) Policies, Procedures, and/or Standards
- (b) Competency Requirements
- (c) Training Requirements
- (d) Documentation Requirements
- (e) Roles and Accountabilities of Departments and Individuals; and
- (f) Compliance Assurance and Auditing Protocols

BP agrees to pay the full amount of the remaining proposed penalties -\$50,610,000.00

Slide 1- 43



## Function Safety Engineering

### Buncefield, UK: 11 December 2005



Slide 1- 44



## Function Safety Engineering

### **Government guidance and the Process Safety Leadership Group (PSLG) Guidance**

- The Buncefield incident investigation team has published eight reports providing findings and recommendations for use within the process industries.
- The report from the PSLG provides guidance on the application of functional safety management system
- Complements existing guidance on Safety Management Systems already provided in the SEVESO directive and other Process Safety Management guidance, regulations and standards

Slide 1- 45



## Function Safety Engineering

**The guidance states that for a Hazard Installation an Functional Safety Management System must be in place and contain for each phase in the Safety Instrumented System lifecycle:-**

- ◆ Safety planning, organisation and procedures;
- ◆ Identification of roles and responsibilities of persons;
- ◆ Competence of persons and accountability;
- ◆ Implementation and monitoring of activities;
- ◆ Procedures to evaluate system performance and validation including keeping of records;

Slide 1- 46

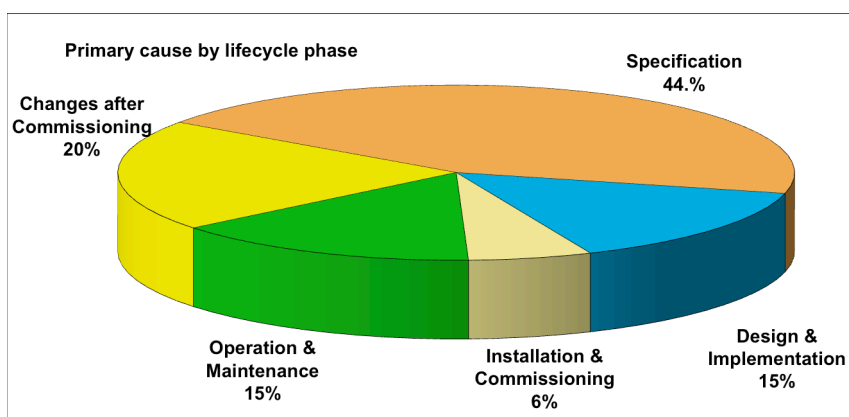
**PSLG Guidance continued:-**

- ◆ Procedures for operation, maintenance, testing and inspection;
- ◆ Functional safety assessment and auditing;
- ◆ Management of change;
- ◆ Documentation relating to risk assessment, design, manufacture, installation and commissioning;
- ◆ Management of software and system configuration

■ The focus of the guidance supports previous HSE research into the causes of systematic failures

Slide 1- 47

**Incidents Caused by Control and Safety System Failures**



HSE UK : "Out of Control" Figure 10 (ISBN 978 0 7176 2192 7)

Slide 1- 48



## HSE Summary: Analysis of Incidents

- Majority of incidents could have been anticipated if a systematic risk-based safety lifecycle approach had been applied
- Safety principles are independent of the technology
- Situations often missed through lack of systematic approach
- Need to verify that the specification has been met
- Over dependence on single channel of safety
- Failure to verify and validate the software
- Poor consideration of human factors
- Inadequate specification of the safety requirements because of :
  - ◆ poor hazard analysis
  - ◆ inadequate assessment of the impact of failure modes of the control system

Slide 1- 49



## Regulatory Compliance

### Every employer **MUST** comply:

- Every employer shall make a **Suitable and sufficient** assessment of the risks to the health & safety of his employees ...and of persons not in his employment
- Every employer shall make and give effect to such risk reduction arrangements as are arrangements **as are appropriate**.....

Slide 1- 50

